SECTION 11. MISCELLANEOUS REGULATIONS

**EffDte: 02/28/1978 MCRT#: 0 Div: D3D9D0RM Cav: SecCls:

11-1 FIELD OFFICE LAW ENFORCEMENT CORRESPONDENCE

**EffDte: 12/12/1991 MCRT#: 0 Div: RM Cav: SecCls:

11-1.1 Deleted

**EffDte: 12/12/1991 MCRT#: 0 Div: PA Cav: SecCls:

11-1.1.1 Deleted

**EffDte: 12/12/1991 MCRT#: 0 Div: PA Cav: SecCls:

11-1.1.2 Deleted

**EffDte: 12/12/1991 MCRT#: 0 Div: PA Cav: SecCls:

11-1.2 Recommendation for Letter from Director (See MAOP, Part 1, 5-17.)

(1) When letters of congratulations, appreciation, or condolence from the Director to individuals other than FBI employees are recommended by the field, such recommendations should be submitted promptly on Form FD-468, not on Form FD-255 (Recommendation for an Incentive Award). Requests should include the following:

(a) Full identifying data, titles, etc., and address of person(s) to be written;

(b) Specific data on which recommendation is based;

(c) Results of field office indices check.

(2) Unless specified, letters are mailed directly from Headquarters to the addressee and no informational copies are made except for requesting office. If the addressee is a superior, other letterhead copies will be provided for each subordinate being commended. Any special circumstances such as the following should be

| noted:

(a) Copy to be sent to addressee's superior;

(b) Letter to be sent back to the field office for presentation;

(c) Any deadline should be noted and highlighted.

(3) If requests involve letters to individuals who reside within another field office's territory, approval should be sought from that office and included in the remarks on the FD-468. For example, when an election of officers of a police association occurs at a convention held in a field office territory, recommendations for congratulatory letters should be submitted by that office. Approval should be sought from the field office where the officer resides and this information should be included in the FD-468.

| (4) FORM FD-468, NOT|ELECTRONIC COMMUNICATIONS,|SHOULD BE USED AS THIS FORM CLARIFIES REQUEST AND EXPEDITES PROCESSING.

(5) REQUESTS SHOULD NOT BE COMBINED WITH FORM FD-255 (Recommendation for Incentive Award).

**EffDte: 06/20/2000 MCRT#: 997 Div: PA Cav: SecCls:

11-2 MAILING LISTS OF FIELD OFFICES

The mailing lists of field offices are compiled at FBIHQ on the basis of information submitted by the various field offices. The SAC will be held responsible for making timely notification to FBIHQ regarding required changes. When a revised mailing list is received from FBIHQ, it is the responsibility of each SAC to ensure that prompt and appropriate changes are made in the office's mailing procedures. Current changes are indicated by an asterisk.

**EffDte: 12/12/1991 MCRT#: 0 Div: D3 Cav: SecCls:

| 11-2.1 |Deleted|

**EffDte: 06/06/1996 MCRT#: 566 Div: D3 Cav: SecCls:

| 11-3 |DELETED|

**EffDte: 06/08/1995 MCRT#: 396 Div: PA Cav: SecCls:

11-4 COPYRIGHT

(1) Copyright laws invest the copyright holder with the exclusive right to control the reproduction and derivative use of the copyrighted material. This protection is extended to "original works of authorship fixed in any tangible medium." Therefore, copyrighted materials are not to be reproduced for internal use or public distribution without the permission of the copyright owner unless such reproduction is allowed by a statutory exception to this general requirement.

(2) The doctrine of "fair use" is a statutory exception most likely applicable to reproduction for noncommercial purposes. Fair use generally permits the reproduction of a portion of copyrighted material without the copyright owner's permission for purposes such as criticism, comment, news reporting, teaching, scholarship, or research. In determining whether the use is fair, factors to be considered are: the purpose of the copying, whether for commercial or nonprofit educational purposes; the portion copied in relation to the whole work; the type of work copied, i.e., books, photographs or charts; the potential diminution of the market or value of the copyrighted work.

(3) Permissible ranges of copying have not been specifically provided for by statutory construction. However, under a rule of reasonableness, a single copying of a chapter of a book; an article from a periodical or newspaper; a chart, drawing, photograph from a book, periodical or newspaper would come within the fair use exception. Copying should be limited to exact need and should not substitute for the purchase of reprints or books from the publisher. Whenever copyrighted material is reproduced, the notice of copyright should be included on the first page of the copied material. The notice of copyright is generally found at the beginning of the book or magazine, and states who holds the copyright and the date of the copyright.

Any specific problems regarding copyright matters should be referred to Administrative Law Unit, Office of the General Counsel, FBIHQ.

**EffDte: 09/09/1994 MCRT#: 281 Div: D9 Cav: SecCls:

11-5 FBIHQ INFORMATION MANAGEMENT POLICY

**EffDte: 12/12/1991 MCRT#: 0 Div: RM Cav: SecCls:

11-5.1 FBIHQ Filing of Documents for Official Records

(1) Federal regulations governing document filing:

To assist FBIHQ officials and supervisors in determining if documents should become part of our official records, the following laws, regulations, policies, and guidelines should be adhered to:

(a) Title 44, United States Code (USC), Section 3101, requires that the head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

(b) Title 44, USC, Section 3102, requires that the head of each Federal agency shall establish and maintain an active, continuing program for the economical and efficient management of the records of the agency. The program, among other things, shall provide for:

1. Effective controls over the creation, and over the maintenance and use of records in the conduct of current business;

2. In cooperation with the Administrator of General Services and the Archivist in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value.

(c) Title 36, Code of Federal Regulations - To ensure that complete and accurate records are made and retained in the FBI, it is essential that we distinguish between records and nonrecord materials by the appropriate application of the above laws.

(2) Documentary materials are records when they meet both the following conditions:

(a) They are made or received by the FBI under Federal law or in connection with the transaction of FBI business; and

(b) They are preserved or are appropriate for preservation as evidence of the FBI organization and activities or because of the value of the information they contain. (If a document is filed for informational purposes only, it should have long-term use. If not, it should only be maintained by the interested party and destroyed when no longer needed.)

(3) The following categories of documents are informational in character and should not be routinely filed as official records:

(a) Teletypes from other Government agencies which provide general intelligence information but do not directly support

| specific investigations, counterintelligence activities, or
| investigative program management.

| (b) VISA teletypes re visitors or immigrants which
| are not relevant to our investigative or counterintelligence
| responsibilities.

| (c) Transmittal Form documents which are of no value
| for recordkeeping purposes.

| (d) Statistical gathering documents (once data is
| loaded into our computer system or captured in other ways, there is no
| need to keep the document).

| (e) "For Information Memo" which doesn't meet the
| criteria of an official record.

| (f) Training and Conference Documents (There should
| be one document which describes the training or conference maintained
| as an official record, but not every teletype to and from field
| offices confirming attendance and containing other administrative
| information should be filed.)

| (g) Negative Request for Agency Check (FD-356)
| Negative FBIHQ Record Checks (FD-493)
| Negative CIA Record Checks (FD-786, 0-66)

| (The field office that requested these checks will have the results.)

**EffDte: 12/12/1991 MCRT#: 0 Div: RM Cav: SecCls:

11-5.2 Bureau Manuals - Making and Transmitting Manual Changes

(1) Manual policy changes are to be accomplished and transmitted to the field in one of the following ways:

(a) By routine manual changes with no advance notification to manual users. (See (3) below.)

(b) By memorandum to all Special Agents in Charge (SAC) followed by manual change. The manual changes should be prepared at the same time as the SAC Memorandum.

(c) Deleted

(d) Policy changes which must be transmitted immediately to manual users may be sent by all-office electronic communications (EC), and policy changes containing highly sensitive information may be transmitted by classified all-office EC. |FBIHQ,|Manuals Desk, MUST appear in the|attention line|of all-office ECs. These are the ONLY approved exceptions to the issuance of policy changes by SAC Memoranda.

(2) Policy changes transmitted by all-office EC are to be followed by a manual change EC directed to the Manuals Desk, |Records Management Division (RMD),|within 10 workdays.

(3) Prior to the submission of a manual change EC and an SAC Memorandum (or all-office EC--see (1)(d)) providing advance notification to FBI personnel, contact should be made with the Manuals Desk for assistance. See Section 14 of the "Correspondence Guide - FBIHQ" for the proper format for making manual changes. Rough drafts of the manual change EC and SAC Memorandum MUST be submitted to the Manuals Desk prior to submitting them to appropriate officials for approval. Ensure a lead is included in the EC AND properly set for the|RMD|so that Manuals Desk has an automated notification of the request. Additionally, the original and any file copies of the manual change EC and the original and file copies of the SAC Memorandum MUST be sent to the Manuals Desk for handling. The manual change EC may be uploaded by the originating division; however, the SAC Memorandum |must|be uploaded ONLY by the Manuals Desk.

(4) Deleted

**EffDte: 08/15/2002 MCRT#: 1074 Div: RM Cav: SecCls:

|11-6 SURVEYS DIRECTED FROM FBIHQ TO FBI FIELD OFFICES

(1) DEFINITION: A survey is defined as any FBIHQ request for information directed to field and/or Legal Attache offices that requires, either on a one-time or recurring basis, the collection of facts, figures, or other data that, when aggregated, are essential in determining the status, value, performance and/or condition of a program, process, policy, system, or other organizational function.

(2) The information provided by surveys may serve any operational, administrative, legal, or quality feedback requirement required by FBIHQ, including information requirements originating from outside the FBI.

(3) The 1983 policy, as provided below, will continue to apply:

(a) A control file will be maintained in each FBIHQ division (separate offices included) to act as a repository for copies of all surveys to the field which originate from that division/office;

(b) Each FBIHQ division/office will designate a manager to oversee this control file and to coordinate, plan, and review all division/office surveys prior to their being forwarded for approval; and

(c) Any standing and periodic surveys approved as to form and frequency may thereafter be disseminated without resubmission

| for approval.

| (4) JUSTIFICATION REQUIREMENTS FOR SURVEYS: In order to ensure that only essential surveys are sent to field offices, all divisions/offices will, when requesting authority to survey the field, provide justification for such requests in accordance with the following guidelines:

| (a) Provide a statement that characterizes the value of the survey, how the information will be used, and the organizational objectives to be attained.

| (b) Certify that the information requested is unavailable from existing FBIHQ information systems or records and that the data collection requirements are worth the time that will be redirected from investigations.

| (c) Certify that only the minimum level of information is being requested to satisfy FBIHQ needs and only from the appropriate field offices.

| (d) Ensure that the survey or request is as concise as possible and provides for ease of use and completion. To accomplish this, the sponsoring component will assure the following:

| 1. Instructions and questions are clearly worded, with consistent formats;

| 2. Uses the most efficient distribution/ collection/processing media (e.g., computer networks);

| 3. Uses standard time frames (e.g., end of fiscal year) when possible;

| 4. Provides a reasonable deadline;

| 5. Provides a contact person/telephone number for questions from the field offices; and

| 6. Provides information feedback to the participating field offices, when appropriate.

| (e) When the survey is approved, the Inspection Division's Organizational Program Evaluation and Analysis (OPEA) Unit will be included on the copy count of the document that transmits the survey to the field.

| (5) OPEA ASSISTANCE:

| (a) OPEA will provide prompt assistance, when requested, in the development of surveys and/or requests for information.

| (b) OPEA will maintain an index of approved surveys, including the topic(s), originating division/office, a general statement of the nature and extent of the targeted respondents, and

| date of the survey. This index will be available to all FBIHQ
| divisions and offices to aid in their search for preexisting data and
| to provide samples of survey questions.

| (6) FINAL APPROVAL: Each survey that meets the terms of
| the above definition will be forwarded to the Deputy Director for
| final approval. The cover communication that transmits the survey
| will contain a specific statement that the survey has been approved by
| the Deputy Director.|

**EffDte: 08/11/1994 MCRT#: 293 Div: D0 Cav: SecCls:

| |11-7 ADMINISTRATIVE USE OF INTERNET/INTERNET ELECTRONIC MAIL (E-MAIL) POLICY AND GUIDELINES

| (1) The Internet is an interconnection of computer networks
| that enables connected machines to communicate directly with one
| another. It connects universities, research labs, and commercial,
| military and government sites around the world. Users of the Internet
| can exchange E-mail as well as send files to one another.

| (2) There has been a surge of interest among FBI employees
| over the past few years to enhance their information and communication
| resources by utilizing the Internet. As the FBI utilizes new forms of
| technology such as the Internet, there is a crucial need for policy
| and guidelines. Set forth are the administrative FBI policy and
| guidelines for Internet E-mail, utilizing the Internet as a research
| tool, and guidelines for providing public information via the
| Internet.

| (3) The following topics are addressed in 11-7.1 through
| 11-7.8:

| (a) GENERAL INFORMATION defines the FBI's
| administrative purpose for using the Internet and user responsibility
| when accessing the Internet.

| (b) INTERNET CONDUCT describes acceptable behavior
| and user expectation when accessing the Internet.

| (c) PRESERVATION OF RECORDS defines a federal
| record, FBI policy for processing and preserving Internet E-mail
| messages, and guidelines for creating E-mail messages.

| (d) INTERNET E-MAIL ACCOUNTS defines an FBI E-mail
| account and provides procedures for obtaining an account.

| (e) SECURITY explains multiuser usage, passwords,
| downloading files to FBI systems and system requirements needed to
| access the Internet.

| (f) PUBLIC INFORMATION explains what type of

| information the FBI can publish on the Internet and Home Pages.

| (g) POINTS OF CONTACT (POC) contains the POC for
| various Internet matters.

| (h) GLOSSARY defines terms used in this document
| which are essential in understanding the administrative Internet
| policy.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.1 General Information

| (1) The FBI will use the Internet to solicit and accept
| Internet E-mail, as a research tool for authorized purposes (See Title
| 5, C.F.R., Section 2635.704(b)(2) and Title 41 C.F.R. Section 128-
| 1.5006-4), and to provide public information on the World Wide Web
| (WWW) (example: press releases, major case information, pamphlets,
| congressional testimonies, job opportunities, Freedom of Information
| and Privacy Act issues and the like).

| (2) Internet policies and guidelines are applicable to all
| FBI employees, federal or state government personnel, contractors, or
| anyone who is granted access to FBI systems.

| (3) Users of FBI systems are individually responsible for
| understanding and respecting Internet policies and guidelines.

| (4) The Security Officer is to ensure compliance with FBIHQ
| security policy for FBI microcomputer systems as contained in the
| MIOG, Part II, 35-9. The points contained in the All SACs Memorandum
| 20-90, dated July 23, 1990, entitled "Security Awareness Training for
| All FBI Employees," must be brought to the attention of all employees
| semiannually. Administrative Internet Policy will be included in this
| briefing (see MIOG, Part I, 261-2).

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

11-7.2 Internet Conduct

(1) Neither the Internet nor the FBI's Internet resources afford individual users any expectation of privacy or confidentiality. Users should understand that the Internet is not a secure medium and all Internet activities and communications are subject to interception/exploitation by unauthorized persons.

(2) The following policy defines the required conduct and expectations of anyone who is granted access to the Internet on FBI systems:

(a) Internet activities involving FBI resources are subject to monitoring (including retrieval and retention) and will be monitored by authorized FBI security, systems, and management personnel (and their authorized Agents). Any use of, or access to FBI resources constitutes consent of such monitoring. (This in no way means that users are free to divulge any information transmitted or received via the Internet. The FBI's requirement that employees must keep all information acquired in their official capacities strictly confidential, applies to Internet communications also, and employees are prohibited from disclosing FBI information to any person or agency not authorized to receive it.) FBI employees are reminded that they should always be mindful of the high standards of behavior expected of them at all times in their personal and official activities (see MAOP, Part 1, Section 1).

(b) Information derived from such FBI monitoring and any violation of subsections (c) through (f), below, involving the use of Bureau mainframe or laptop computers, may serve as a basis for administrative, disciplinary, or legal proceedings if evidence illustrates that an employee is involved in illegal or improper activities which violate federal or state laws, regulations, or FBI policies.

(c) Use of the Internet is a privilege, not a right, which may be revoked at any time for inappropriate conduct. The following are examples which will cause the user's access to be revoked: use of the Internet for unlawful or malicious activities; abusive or objectionable language in either public or private messages; browsing sexually explicit sites and chat rooms, or transmitting or forwarding sexually explicit material through Internet or FBI e-mail systems; misrepresentation of oneself or the FBI; sending chain letters; other activities that could cause congestion and disruption of networks and systems.

(d) Users will not knowingly engage or participate in any activity that causes harm to the FBI (i.e., creating or procreating viruses, loading, downloading unofficial software or shareware, unauthorized access to other systems, or any other unlawful or improper act).

(e) Users will not discuss or transmit sensitive or classified information on the Internet or within Internet E-mail messages.

(f) Users will not create or transmit materials that violate federal or state regulations; or promote discrimination on the basis of race, creed, color, gender, religion, disability, or sexual orientation.

**EffDte: 01/25/2002 MCRT#: 1203 Div: D4 Cav: SecCls:

| 11-7.3 Preservation of Records/Processing Mail

| (1) The FBI is required by law to preserve federal records according to Federal Records Act (FRA) 44 United States Code, Chapters 31 and 33. Federal regulations from the National Archives and Records Administration (NARA), in concert with FBI policy, govern the life cycle of these records which includes storage, preservation, retrieval, and disposition schedules.

| (2) E-mail messages, attachments and essential transmission data are federal records when they meet the criteria defined in the following Federal Records Act.

| WHAT CONSTITUTES A RECORD: Federal records include all books, papers, maps, photographs, machine readable material, or other documentary materials, regardless of physical form or characteristic, made or received by an agency of the United States government under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government or because of the informational value of data in them.

| WHAT CONSTITUTES A NONRECORD: A nonfederal record is information that is not categorized as a federal record and does not require retention beyond its useful life as determined by the originator and/or recipient. Nonrecord information may be purged or destroyed when the information has served the purpose for which it was intended. The following examples, while not all inclusive, illustrate types of nonrecord information: (1) Informal notes and cover notes that are merely informative in nature. (2) Working papers and drafts which have not been approved and are subject to review. (3) Informative notes, communications or documents which an approving official decides should not go to file. (4) Information that is preserved for reference only. (5) Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are included as nonrecords (Title 44, United States Code, Section 3301).

| (3) The following policy and guidelines will be used when processing incoming and outgoing Internet E-mail:

| (a) Internet E-mail, attachments and essential transmission data will be processed like incoming mail from the United States Postal Service (USPS). Once an Internet message is received, it should be (to include but not necessarily inclusive) searched in indices, distributed to correct personnel to determine what classification, file or control file to which the Internet E-mail message should be saved (if a federal record), and follow the current saving and destruction policy (see MAOP, Part II, 2-2.1 through 2-4.3).

| (b) The sender of an outgoing Internet E-mail message

| or attachment that has been deemed a federal record must determine to
| which classification, file or control file the outgoing Internet E-
| mail message should be saved. This is also required of the sender
| when sending a message or attachment that is deemed a federal record
| via the Internet to another Bureau employee.

| (c) Internet E-mail messages and transmission data can
| be easily uploaded into the ECF component of ACS because messages are
| usually in electronic format. If this data is loaded into the ECF
| component of ACS, this information is retrievable by Case ID,
| attributes, serial or full text. Although E-mail messages are usually
| in electronic format, attachments could be in another format such as
| graphics which are not viewable in any component of ACS. Those
| attachments should be printed (if possible), serialized and placed in
| a paper file. Use current FBI policies to determine if these records
| should be loaded into additional FBI applications such as CLEA, IIIA,
| and/or the Telephone Application, etc. Note: All files and programs
| that are downloaded to FBI systems from the Internet or from any
| outside sources must be to a standalone computer or to a floppy disk,
| approved by the Computer Specialist or Security Officer and scanned
| for viruses prior to introduction to any other FBI computer (see
| 11-7.5 "Security").

| (d) Check incoming Internet E-mail daily. Internet
| E-mail should be checked more frequently if warranted by the volume of
| mail received.

| (e) Because of the impact on the FBI's reputation and
| credibility, messages that are deemed federal records that the user
| creates and disseminates should be stated in an intelligible, concise
| and professional manner. Obtain necessary approval as required by
| your division before sending a message.

| (f) Some systems have limitations on the number of
| characters in a message. Therefore, keep outgoing Internet E-mail
| messages short and limited to one subject, if possible.

| (g) Because of software and graphic constraints,
| attachments in Internet E-mail messages should be avoided where
| possible. Some systems are not compatible and difficulty could result
| when reviewing messages and files.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4RM Cav: SecCls:

| 11-7.4 Internet E-mail Accounts

| (1) Every FBIHQ division and field office has an FBI
| Internet account. Some FBI employees have an individual FBI Internet
| E-mail account to be used for official FBI business.
| In this document, Internet E-mail accounts are any Internet E-mail
| accounts that are paid for by the FBI (does not include
| investigative, covert, or other specialized investigative accounts).

| For example: Fieldoffice@FBI.GOV; FBIAcademy.EDU;
| AnyUsersName@FBI.GOV; HQDivision@FBI.GOV and so forth.

| (2) The following procedures will be used in obtaining an
| individual Internet E-mail account:

| (a) E-mail accounts will be granted to users that can
| provide a sufficient justification to the SAC or appropriate authority
| in the division or field office. Notify IRD of any existing or new
| accounts granted, for IRD inventory purposes.

| (b) If approval is granted, you must meet system
| requirements and obtain funding for system requirements and/or funding
| for the account if necessary (see EC titled "Internet Account
| Distribution/Guidelines" dated February 28, 1997).

| (c) FBI.GOV Internet E-mail accounts will be
| reevaluated monthly by IRD to determine if users have maintained a
| need for the account. The account will be terminated within 90 days
| for nonuse. Non-FBI.GOV E-mail accounts that are paid for with FBI
| funds should also be reevaluated monthly and terminated within 90 days
| for nonuse.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.5 Security (See MAOP, Part II, 11-7.3.)

| The following policy describes what is required to avoid
| potential abuse of the Internet and to provide accountability when
| accessing the Internet on FBI systems.

| (1) At a minimum, Watchdog software or a similar software
| package will be used to track usage on "multiuser" FBI Internet
| systems. The following illustrates the type of audit trail with the
| minimum information that must be captured to facilitate reconstruction
| of events if compromise or unauthorized activities occur: user name,
| date, time on and off the Internet (see MIOG Part II, 35-9.3.1).

| (a) Watchdog or a similar software requires each user
| be assigned a unique ID and will also require the user to create a
| password, to be used with the ID for authentication. The ID may be
| publicly known, but passwords must be kept secret.

| (b) Contact your Computer Specialist for access to the
| Internet or if you forget your Watchdog (or similar software) password
| and ID.

| (c) Contact your Computer Specialist or Security
| Officer immediately to report security violations or misuse (see
| MIOG, Part II, 35-9.3.1).

| (2) The following system requirements (not necessarily

| inclusive) are necessary to access the Internet: standalone computer
| (486 or higher), 28kbps (or higher modem), Windows 3.1 or Windows 95,
| 8MB RAM recommended and 6 MB free hard disk space. The hard drive
| must never have been used for FBINET or sanitized using Norton
| Utilities Disk Wipe Government Version. For detailed information see
| EC titled "Internet Account Distribution/Guidelines" dated
| February 28, 1997.

| (3) All files and programs that are downloaded to FBI
| systems from the Internet or from any outside source must be to a
| standalone computer or to a floppy disk, approved by the Computer
| Specialist or Security Officer and must be scanned for viruses prior
| to introduction to any other FBI computer (see MIOG, Part II,
| 35-9.4.4).

| (4) Users are reminded that the Internet is not a secure
| medium and all Internet activities and communications are subject to
| interception/exploitation by unauthorized persons.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.6 Public Information

| (1) In general, per the news media guidelines, FBIHQ
| provides public information regarding national and international
| matters. Field offices provide local public information. Field
| offices are authorized by the Director to make more wide-ranging
| statements on a case-by-case basis.

| (2) In regard to the Internet, the Office of Public and
| Congressional Affairs (OPCA) oversees the content and appearance of
| official FBI material on the web. Prior to placement on the FBI Home
| Page, FBI matters must be reviewed and approved by the National Press
| Office (NPO) and the OPCA, with concurrence of other appropriate FBIHQ
| divisions, as needed. This is to ensure consistency with current FBI
| and DOJ policy and guidelines. (See MAOP, Part II, 5-10.)

| (3) FBI field offices may request their own Home Page
| accessible through the FBIHQ Home Page. Field offices are responsible
| for submitting their respective Field Office Home Page information and
| ensuring that information is updated as needed via the NPO and OPCA.
| OPCA is responsible for placement, removal, and updating of official
| FBI material on the WWW/FBI Home Page. The sole purpose of this
| process is to ensure consistency on national issues and compliance
| with DOJ guidelines.

| (4) Submit information for a Field Office Home Page to the
| NPO and OPCA. Information should be local in nature and avoid
| repetition of information included on the FBIHQ Home Page. Submit
| information on a computer disk, in WordPerfect or Freelance programs,
| ASCII format, with or without formatting instructions, and include a
| paper copy. For detailed information, see Airtel titled, "Policy For

| Publishing FBI Information On The World Wide Web" dated September 22,
| 1995.

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.7 Internet Points of Contact

| Contact the division or unit below on the following Internet
| issues if you have any questions:

ISSUE	DIVISION AND/OR UNIT
Legal:	Office of General Counsel, Administrative Law Unit
	Chief Division Counsel
Home Page:	Office of Public and Congressional Affairs, Press Office
System Requirements:	Information Resources Division, Investigative Applications Support Unit
Noninvestigative Accounts:	Information Resources Division, Investigative Applications Support Unit
Investigative Accounts:	Criminal Investigative Division, Corruption/Civil Rights Section, Undercover and Sensitive Operations Unit
(Major Cases)	National Security Division, Special Surveillance Group (SSG), FCI/CT Lookout & Undercover Support Unit (NS-5D)

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

| 11-7.8 Glossary

ACS	Automated Case Support.
Appropriate authority	In this document, appropriate authority refers to FBIHQ or field office management (i.e., Section Chief or higher at FBIHQ; SAC in the field office).
Authorized Purposes	Those purposes for which government property is made available to the public or purposes authorized in accordance with law or regulation

	(see Title 5, C.F.R., Section 2635.704(b)(2)).
CFR	Code of Federal Regulations.
Download	To transmit a file or program from a central computer to a smaller computer or a computer at a remote location.
ECF	Electronic Case File. A component of ACS. ECF serves as the central electronic repository for the FBI's official investigative textual documents. ECF provides the capability to upload word processing documents to the mainframe, where they are then filed and serialized.
Electronic Mail	Also referred to as E-mail, is the most frequently used communications tool on the Internet. E-mail are messages that are sent by computer from one person to another, then saved until the recipient chooses to read them. E-mail arrives immediately and does not require the recipient to be present, nor does it interrupt anything else the recipient may be doing.
FRA	Federal Records Act.
Internet	The Internet is an interconnection of computer networks that enables connected machines to communicate directly with one another. It connects universities, research labs and commercial, military and government sites around the world. Users of the Internet can exchange E-mail as well as send files to one another.
Internet Account	In this document, any Internet account that is paid for by the FBI (does not include accounts used in investigative, covert, or other specialized investigative uses).
Multiuser	When more than one user accesses the same FBI system or account.
NARA	National Archives and Records Administration.
Password	A secret character string that is required to log onto a computer system, thus preventing unauthorized individuals from obtaining access to the computer. Passwords are used to authenticate.
Research	Research, in this document, refers to the collection and maintenance of publicly accessible information for job-related purposes

	but does not include the collection and maintenance of information that is intended to be covert or that which is related to any other specialized investigation that requires authorization from an FBI official.
Sensitive Information	Information that requires protection due to the risk or magnitude of loss or harm that could result from inadvertent or deliberate disclosure, modification and/or destruction of information. Also referred to as Sensitive but Unclassified Information and Limited Official Use Information. (See MIOG, Part II, 35-12.)
Transmission Data	Sometimes referred to as Receipt Data. Can include information such as the date and time message was sent, date and time message was read, acknowledgment by recipient and the identities of senders and recipients. For messages where senders/recipients are identified by "handle" or distribution list, address group, or the like, the means to identify the associated names must also be included.
USPS	United States Postal Service.
WWW	World Wide Web. The entire constellation of resources that can be accessed by Gopher, FTP, HTP, WAIS and other search tools.|

**EffDte: 11/17/1998 MCRT#: 845 Div: D4 Cav: SecCls:

********** END OF REPORT **********